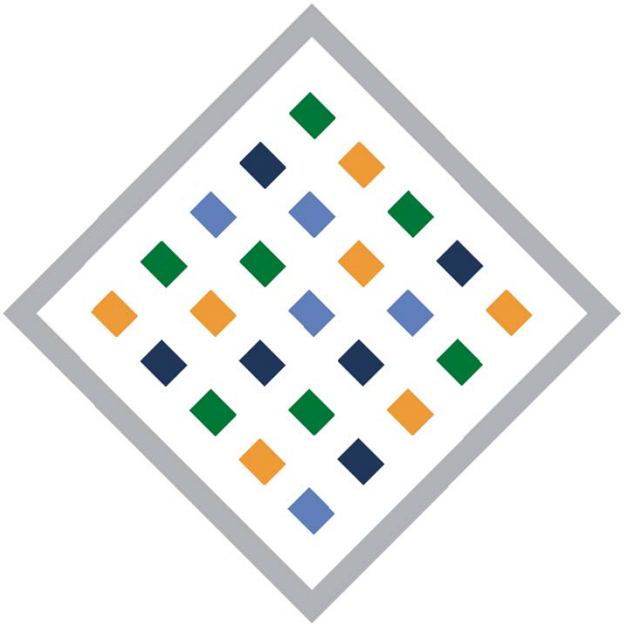
6. Stralsunder IT-Sicherheitskonferenz



Von Smartphone bis Smarthome - Datenschutz im „Internet der Dinge“

Thomas Brückmann

Referent

beim Landesbeauftragten für Datenschutz und Informationsfreiheit

Mecklenburg-Vorpommern

Agenda

1. Datenschutz?
   - Wer wir sind und was wir machen
2. Definition des IoT
3. Rechtsgrundlagen
   - Die aktuelle Rechtsgrundlage
   - Die zukünftige Rechtsgrundlage
   - Was ist zu tun?
4. Gefahren und Beispiele
5. (Kurz-)Fazit / ToDo‘s

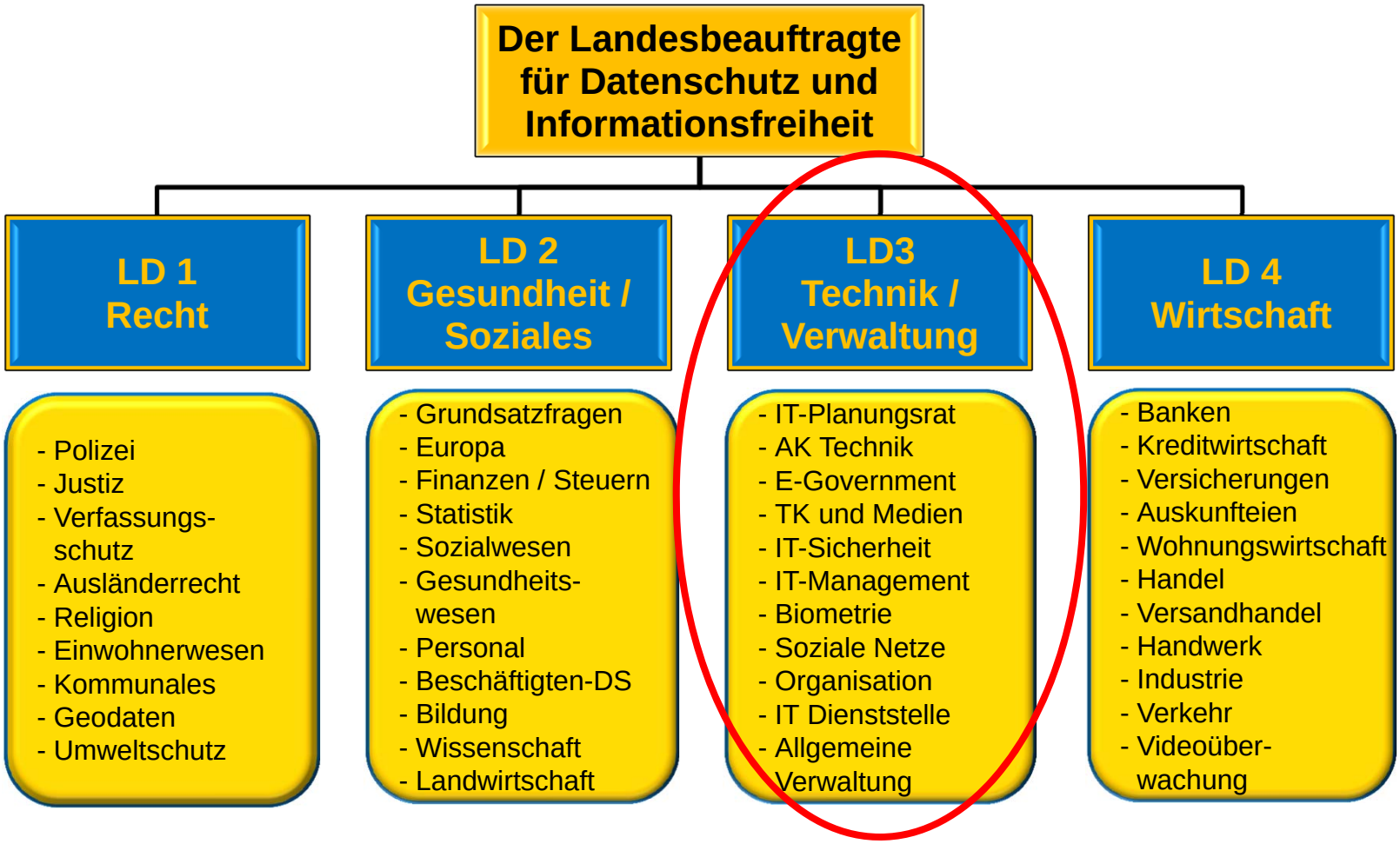
Rechtsstellung der Landesdatenschutzbeauftragten

- Wahl durch das Parlament (6 Jahre Amtszeit)
- Organisatorische Anbindung bei Landtagspräsidentin
- Unabhängig und weisungsfrei (keine Fach- oder Rechtsaufsicht seit 2011; Dienstaufsicht der Landtagspräsidentin nur soweit Unabhängigkeit nicht tangiert)
- Oberste Dienstbehörde i. S. v. § 96 StPO u. Oberste Aufsichtsbehörde i. S. v. § 99 VwGO

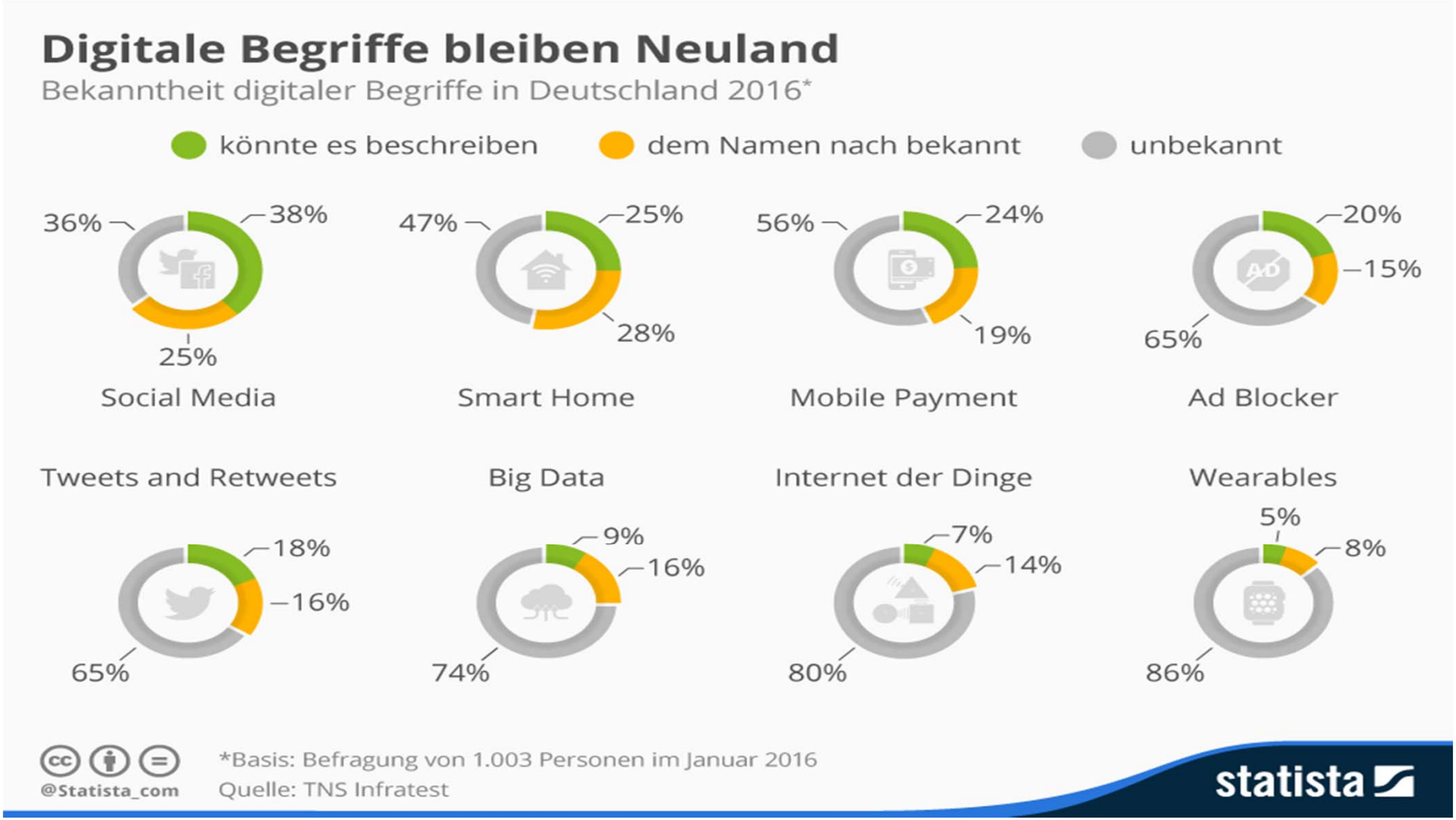
Aufgaben und Befugnisse des Landesbeauftragten

- Bearbeitung von Petitionen
- Beratung bei der Erarbeitung von Gesetzentwürfen
- Kontrolle der Einhaltung gesetzlicher Vorschriften
- Beratung von Behörden und Unternehmen
- Erarbeitung von Gutachten
- Information der Öffentlichkeit
- Zusammenarbeit mit anderen Datenschutzinstitutionen
- Beobachtung der Entwicklung der IuK-Technik
- ...

Das Amt des LfDI M-V



Internet der Dinge



Internet der Dinge???

Der *Versuch* einer Definition:

Mark Weiser 1991: „**The Computer for the 21st Century**“

Intelligente Gegenstände („smart things“) ersetzen den Computer und unterstützen ohne aufzufallen oder abzulenken.

„Im 21. Jahrhundert wird die technologische Revolution das Alltägliche, Kleine und Unsichtbare sein.“

Aufgaben von UC-Systeme

- stetig und überall verfügbare Computerunterstützung („ubiquitär“)
- stark vereinfachte Schnittstellen zwischen Mensch und Computer, welche die Aufmerksamkeit und Interaktion der Nutzer minimal einfordern („Calm Computing“)
- automatische Steuerung und Anpassung der Umgebung an Nutzerpräferenzen oder situative Kontexte
- automatische Ausführung und Abwicklung wiederkehrender standardisierter Abläufe ohne Einforderung einer Nutzerinteraktion

Komponenten von UC-Systeme

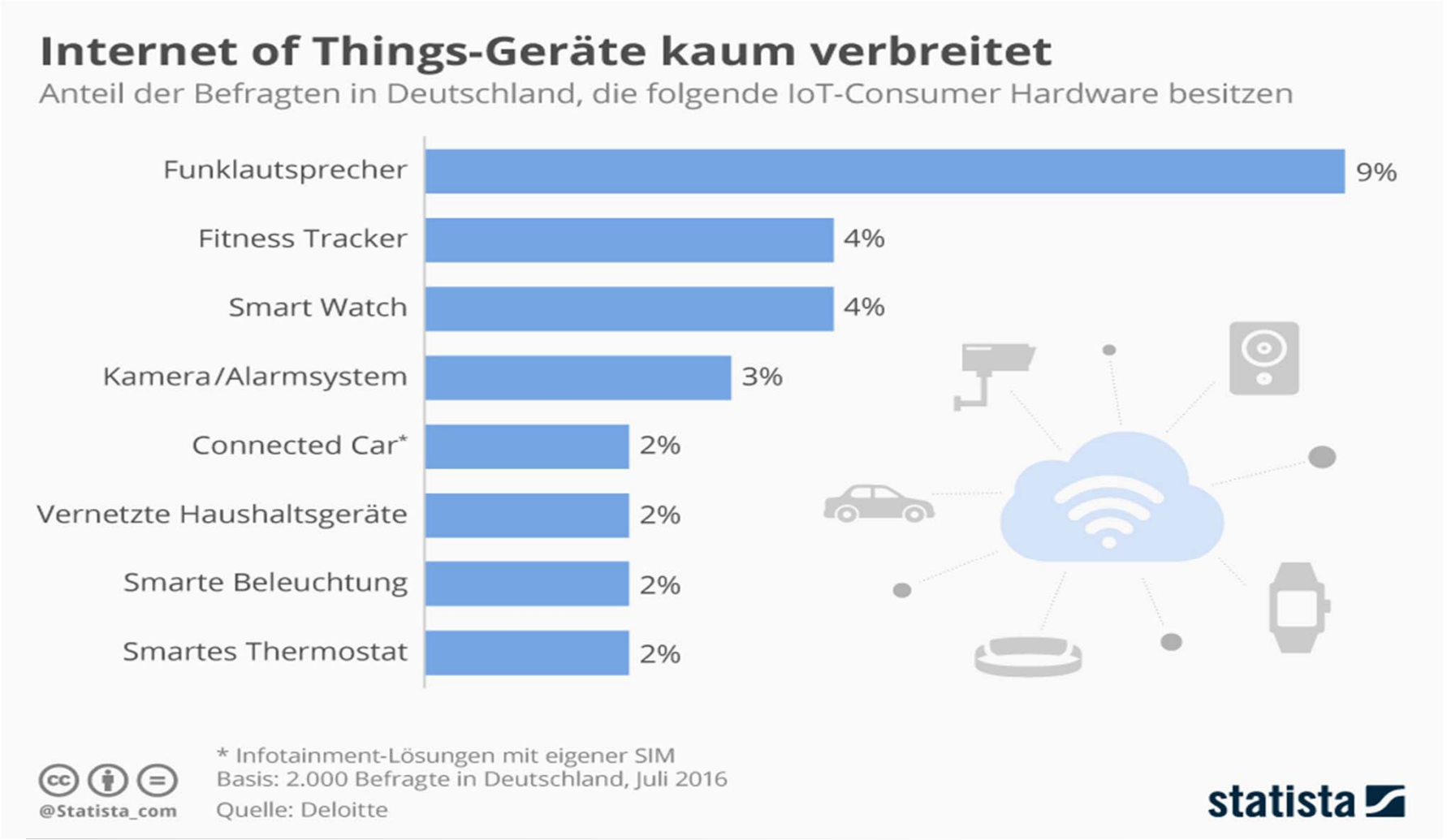
- verteilte Infrastruktur für Sensoren und Schnittstellen (Interfaces)
- verteilte Infrastruktur für Transport von Daten
- Rechenleistung von einem oder mehreren (verteilten) Computern, die Daten verarbeiten und Entscheidungen treffen
- Zugriff auf einen oder mehrere (verteilte) Datenspeicher
- Anbindung an externe Datenquellen und Dienste
- Komponenten zur Umsetzung von Entscheidungen bzw. zur Ausführung einer Dienstleistung (Service) oder anderen Aktionen, ggf. auch in einer verteilten Infrastruktur

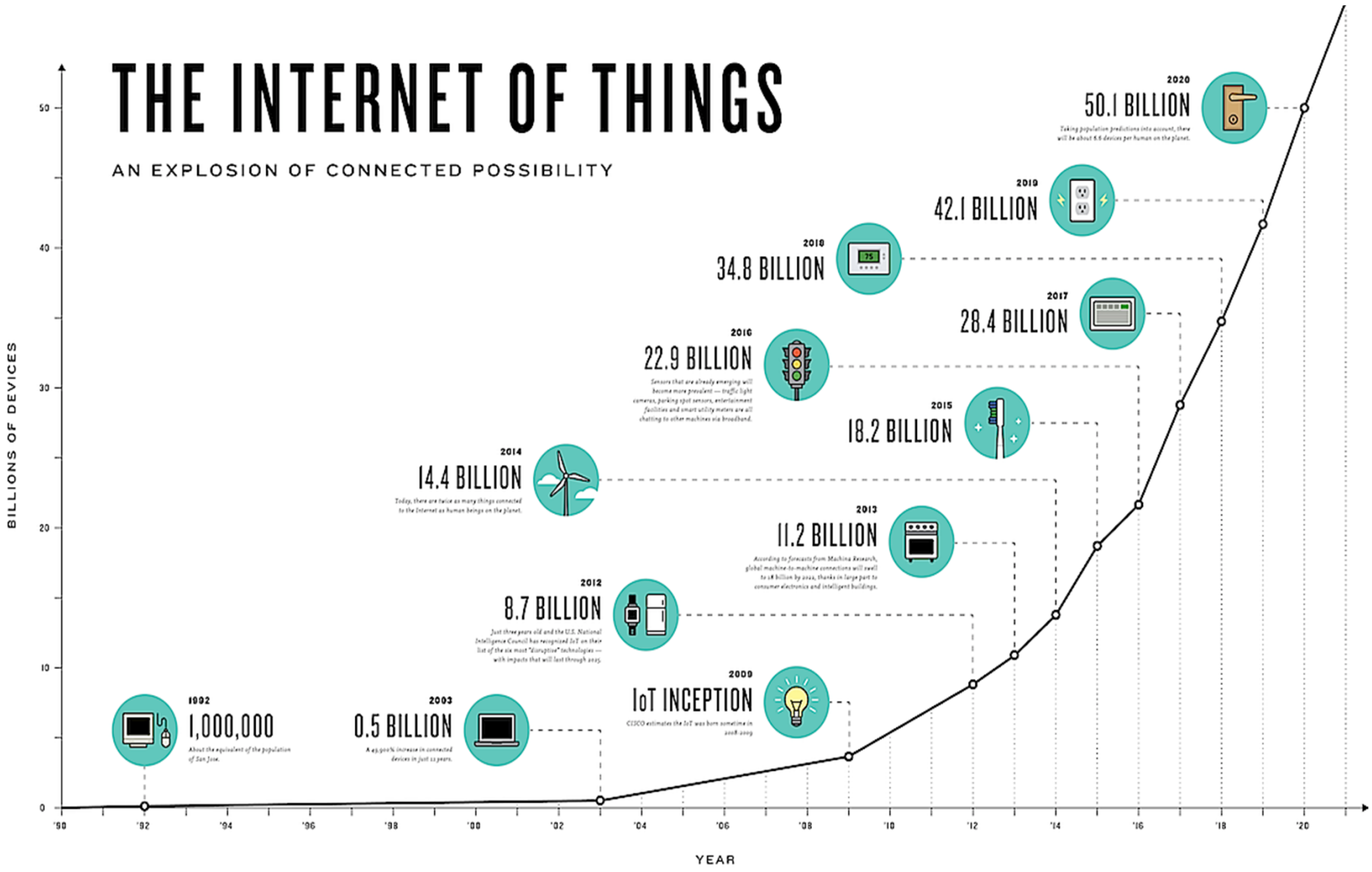
Datenschutz bei UC

Vorhersagen von Mark Weiser:

- ReceptionistIn weiß jederzeit wo sich Leute befinden, Terminals wissen wer vor ihnen sitzt und kennen die Präferenzen, Kalender schreiben sich selbst
- 100erte Computer in einem Raum: Gefahr von totalitärem System
- Regierung und Marketingfirmen nutzen Informationen
- better Privacy durch „digital pseudonyms“
- „build computer systems to have the same privacy safeguards as the real world…“

Internet der Dinge





http://www.i-scoop.eu/internet-of-things/

aktuelle Rechtslage

Quelle: Pixabay

Rechtsgrundlagen

Grundgesetz

Artikel 1
(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung allerstaatlichen Gewalt.

Artikel 2
(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.
(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

EU-Grundrechte-Charta

Artikel 1 - Würde des Menschen
Die Würde des Menschen ist unantastbar. Sie ist zu achten und zu schützen.
Artikel 8 - Schutz personenbezogener Daten
(1) Jede Person hat das Recht auf *Schutz der sie betreffenden personenbezogenen Daten*.
(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit *Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage* verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
(3) Die Einhaltung dieser Vorschriften wird von einer *unabhängigen Stelle überwacht*.

Das Grundrecht auf informationelle Selbstbestimmung – das Volkszählungsurteil

Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983:

Das Grundrecht auf informationelle Selbstbestimmung leitet sich ab aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs.1 GG.

Das Grundrecht gewährleistet die **Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.**

Das Grundrecht auf informationelle Selbstbestimmung – das Volkszählungsurteil

„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann bei welcher Gelegenheit über sie weiß.“

Das bedeutet: Wir leben nicht mehr in einem modernen Rechtsstaat, wenn wir die Kontrolle über unsere Daten verlieren.

BVerfG Volkszählungsurteil 1983 – noch zeitgemäß ?

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht)

Dieses Recht schützt den Betroffenen vor Zugriffen auf **informationstechnische Systeme** wie Computer, Netzwerke und vergleichbare Systeme, wenn diese Zugriffe sein Persönlichkeitsrecht gefährden.

Reaktion des BVerfG am 27. Februar 2008 auf die im nordrhein-westfälischen Verfassungsschutzgesetz (VSG) vorgesehene Online-Durchsuchung.

aktuelle Rechtslage

	öffentliche Verwaltung	„nicht-öffentlicher“ Bereich § 2(4)	Privatpersonen
Europa	Verordnung(EG) Nr. 45/2001	RL 95/46/EG	
Bund	1. spez. Bundesgesetze 2. §§ 1-26 BDSG	1. spez. Bundesgesetze 2. §§ 1-11, 27ff. BDSG	
Land	1. spez. Bundes- 2. und spez. Landesgesetze 3. DSG M-V	1. spez. Bundesgesetze, sonst 2. BDSG	§ 1 (2) Nr.3 BDSG
Kreis/ Gemeinde			

Warum geht überhaupt alles?

Grundtenor: Verbot mit Erlaubnisvorbehalt!

Lösung: informierte Einwilligung § 4a(1) BDSG, § 7 DSG M-V

- Wirksamkeit setzt **Einsichtsfähigkeit** voraus, d.h. Fähigkeit, Tragweite und Folgen der Erklärung abzuschätzen
- Hinweis auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung

- Formen der Einwilligung:
  1. Ausdrücklich, schriftlich (Regelfall)
  2. Konkludent (durch schlüssiges Verhalten)
  3. Mutmaßlich (nur als (begründete) **Ausnahme** möglich)

Die aktuelle Lage

Amtsblatt der Europäischen Gemeinschaften

Nr. L 281/31

23. 11. 95

DE

RICHTLINIE 95/46/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 24. Oktober 1995

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

Die Lösung am 25. Mai 2018???

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung – DS-GVO)

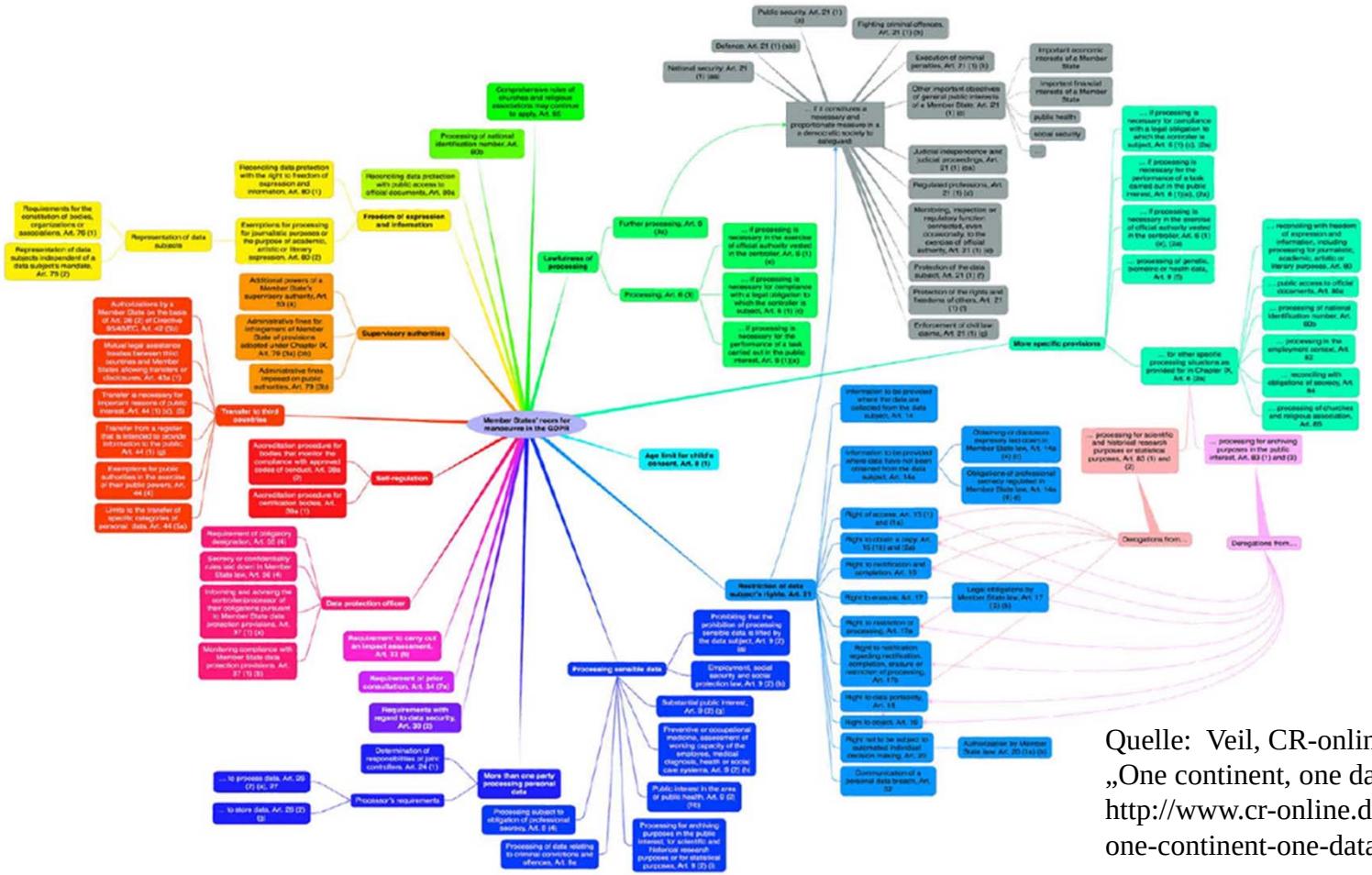
Parlamentum Europaeum

Europäische Kommission

einige Ziele der DS-GVO

- **Kontrolle** über Daten im Sinne der digitalen Grundrechte
- **globale Standards** für Datenschutz
- **Optimierung des modernen digitalen Binnenmarktes**
  - **Harmonisierung** (EUR 2,3 Milliarden Einsparungen durch Vereinheitlichung unterschiedlicher Datenschutzregeln)
  - **Vereinfachung** (EUR 130 Millionen Einsparung durch Abschaffung von Meldepflichten)
  - **kein „Forum-Shopping“** (Datenverarbeitung in Mitgliedsstaat mit weniger strengem Datenschutzrecht)
  - **„One-Stop-Shop“** (eine zuständige Aufsichtsbehörde für Unternehmen in der Europäischen Union)
  - **Kooperationverpflichtung** der Datenschutzaufsichtsbehörden
  - **Konsistenz** der Anwendung des Datenschutzrechts

Öffnungsklauseln - Überblick



Quelle: Veil, CR-online 1. Februar 2016 „One continent, one data protection law?“ http://www.cr-online.de/blog/2016/ 02/01/ one-continent-one-data-protection-law/

Grundsätze für die Datenverarbeitung – Art. 5

„(1) Personenbezogene Daten müssen
a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, ***Transparenz***“);
b) für ***festgelegte, eindeutige und legitime Zwecke*** erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken (***„Zweckbindung“***);
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (***„Datenminimierung“***);
d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, ***unverzüglich gelöscht oder berichtigt werden („Richtigkeit“)***;“

Grundsätze für die Datenverarbeitung – Art. 5

„(e) ***in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist***; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden (**„Speicherbegrenzung“);**
f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („***Integrität und Vertraulichkeit***“);
(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („***Rechenschaftspflicht***“).“

Was tun im Datenschutz-Dschungel?

Quelle: Lizzard / Pixelio.de

Standard-Datenschutzmodell (SDM)

heise online > News > 2015 > KW 40 > Datenschützer verabschieden neues Prüfmodell

« Vorige | Nächste »

Datenschützer verabschieden neues Prüfmodell

heise online 01.10.2015 14:13 Uhr – Christiane Schulzki-Haddouti vorlesen

(Bild: BSI)

Die Datenschutz-Aufsichtsbehörden von Bund und Ländern empfehlen, das Standard-Datenschutzmodell anzuwenden. Dieses unterstützt ein strukturiertes Prüfen von IT-Prozessen, was bisher mangels eines eigenen Prüfmodells nicht möglich war.

- Regelungskern: 7 Schutzziele

- Verfahrenskomponenten: Daten, IT-Systeme, Prozesse

- 3 Schutzbedarfsabstufungen, formuliert aus **Betroffenenperspektive**

- Referenzkatalog mit Schutzmaßnahmen

- 92. DSB-Konferenz hat SDM-Handbuch am 9. November 2016 zustimmend zur Kenntnis genommen (einstimmig bei Enthaltung Bayerns)

siehe: **https://www.datenschutz-mv.de**

Gewährleistungsziele

* **Datensparsamkeit** / Reduzierung erfasstet Attribute betroffener Personen und der Verarbeitungsoptionen / Reduzierung der Möglichkeiten der Kenntnisnahme vorhandener Daten
* **Verfügbarkeit** / Redundanz, Backup und Restore / Vertretungsregeln
* **Integrität** / technischer Integritätsschutz (elektronische Signaturen und deren Prüfungen) / Soll-Definitionen für Prozesse, mit Ereignisdefinitionen zur Prüfbarkeit von Soll-Abweichungen / Prüfsummen / Einschränkung von Schreib- und Änderungsrechten
* **Vertraulichkeit** / Verschlüsselung von Datenbeständen und Kommunikationen / Berechtigungen- & Rollenkonzept
* **Nichtverkettbarkeit** / Trennung / Isolierung unter der inhaltlichen Maßgabe der Umsetzung informationeller Gewaltenteilung / Anonymisierung / Pseudonymisierung
* **Transparenz** / Spezifikation von geplanten Systemen / Dokumentation, die eine Prüffähigkeit von Ist-Zuständen und Soll-Vorgaben erlaubt / Protokollierung von Prozess-Ereignissen / Auskunft
* **Intervenierbarkeit** / Berichtigung, Sperrung, Löschung, Widerspruch („Außenschnittstelle“ einer Organisation) / Prozesse einer Organisation zur Erkennung und Bearbeitungen von Störungen, Problembearbeitungen und Änderungen („Changemanagement“)

Grundsätze für die Datenverarbeitung – Art. 5

Art. 5 Abs. 1 „Personenbezogene Daten müssen“	**Schutzziele:**
(a) „... in einer für die Person nachvollziehbaren Weise verarbeitet werden ... (**Transparenz**).“	**Transparenz**
(b) „... für festgelegte eindeutige und legitime Zwecke erhoben werden ... (**Zweckbindung**).“	**Nicht-Verkettbarkeit**
(c) „... auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (**Datenminimierung**).“	**Datensparsamkeit**
(d) „... damit personenbezogene Daten, die im Hinblick auf die Zwecke der Verarbeitung unrichtig sind, ... **unverzüglich gelöscht oder berichtigt** werden.“	**Intervenierbarkeit**
(f) „... **Integrität und Vertraulichkeit**“.	**Integrität und Vertraulichkeit**

Es fehlt: **Verfügbarkeit ???**

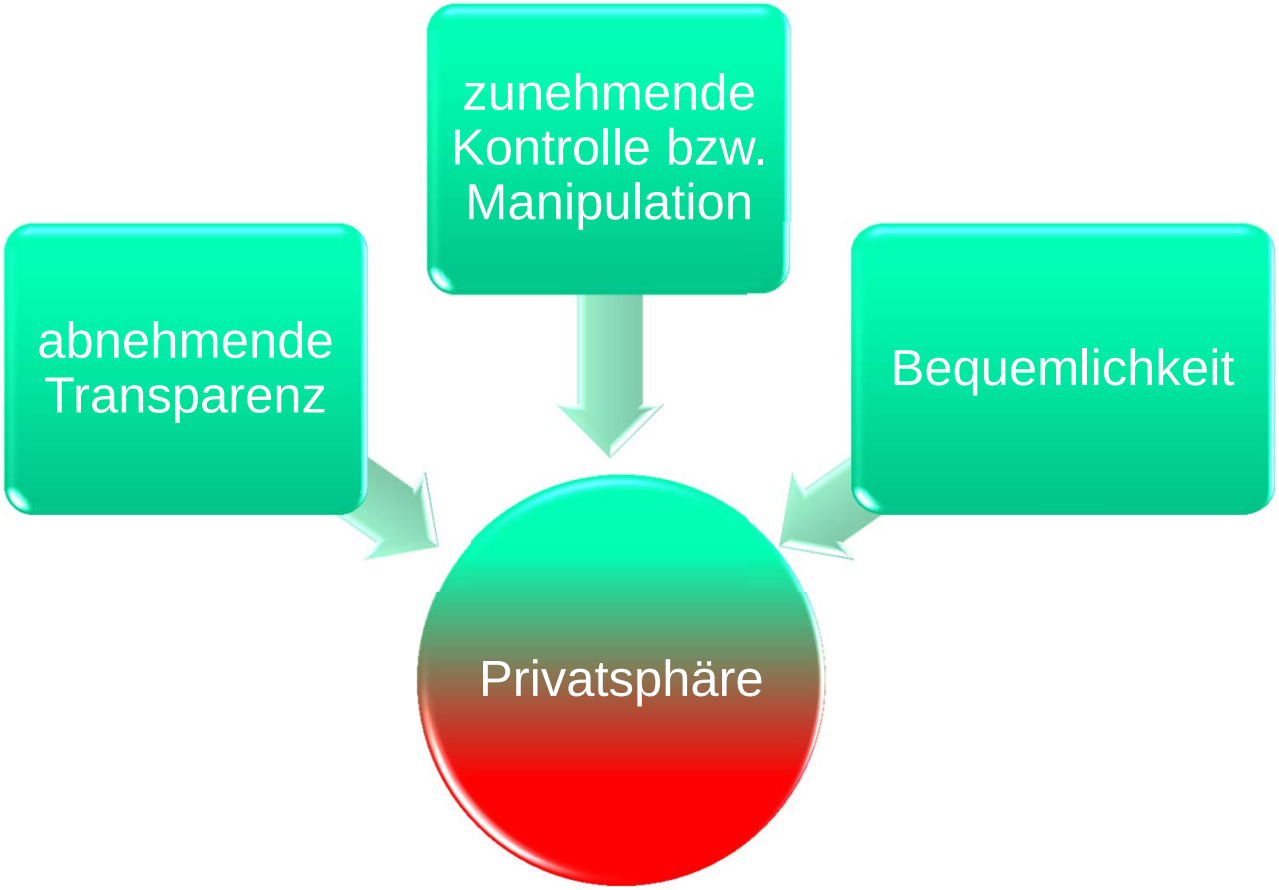
Mapping SDM-Schutzziele und DSGVO

Schutz-ziele:	Datenspar-samkeit	Verfügbar-keit	Integrität	Vertraulich-keit	Nichtver-kettbarkeit	Transparenz	Intervenier-barkeit
Artikel der DS-GVO:	5c/e, 25	13, 15, 20, 25, 32	5d,f, 25, 32	5f, 25, 28/3b, 32	5b, 25, 32	5a, 12, 13, 14, 15, 25, 32, 33, 34	12/2, 15e, 16, 17, 18, 19, 20, 21, 22/3, 25, 28/3g

Gefahren für den Datenschutz

Quelle: Pixabay

Risiken für das Grundrecht „Privatsphäre“



Zwei Jahre digitale Agenda: "Cloud hört sich an wie Stehlen"

heise online 06.09.2016 19:10 Uhr – Stefan Krempl

vorlesen

Thomas de Maizière, Sigmar Gabriel und Alexander Dobrindt bei eco. (Bild: heise online, Stefan Krempl)

Die drei federführenden Minister der digitalen Agenda sind sich einig, dass das Prinzip der Datensparsamkeit weg muss. Das Thema Datensicherheit sei eines der großen Digitalisierungshemmnisse für kleine und mittlere Unternehmen.

CHRISTIAN LINDNER

DIGITAL FIRST. BEDENKEN SECOND.

DENKEN WIR NEU.

Freie Demokraten

FDP

Ich habe doch nichts zu verbergen…

hinter dem Bildschirm

vor dem Bildschirm

Vorsicht vor dem Ungleichgewicht von Geheimnissen !!

Geheimnisse

hinter dem Bildschirm

vor dem Bildschirm

Privatsphäre ist das Instrument, Machtverhältnisse zu balancieren !

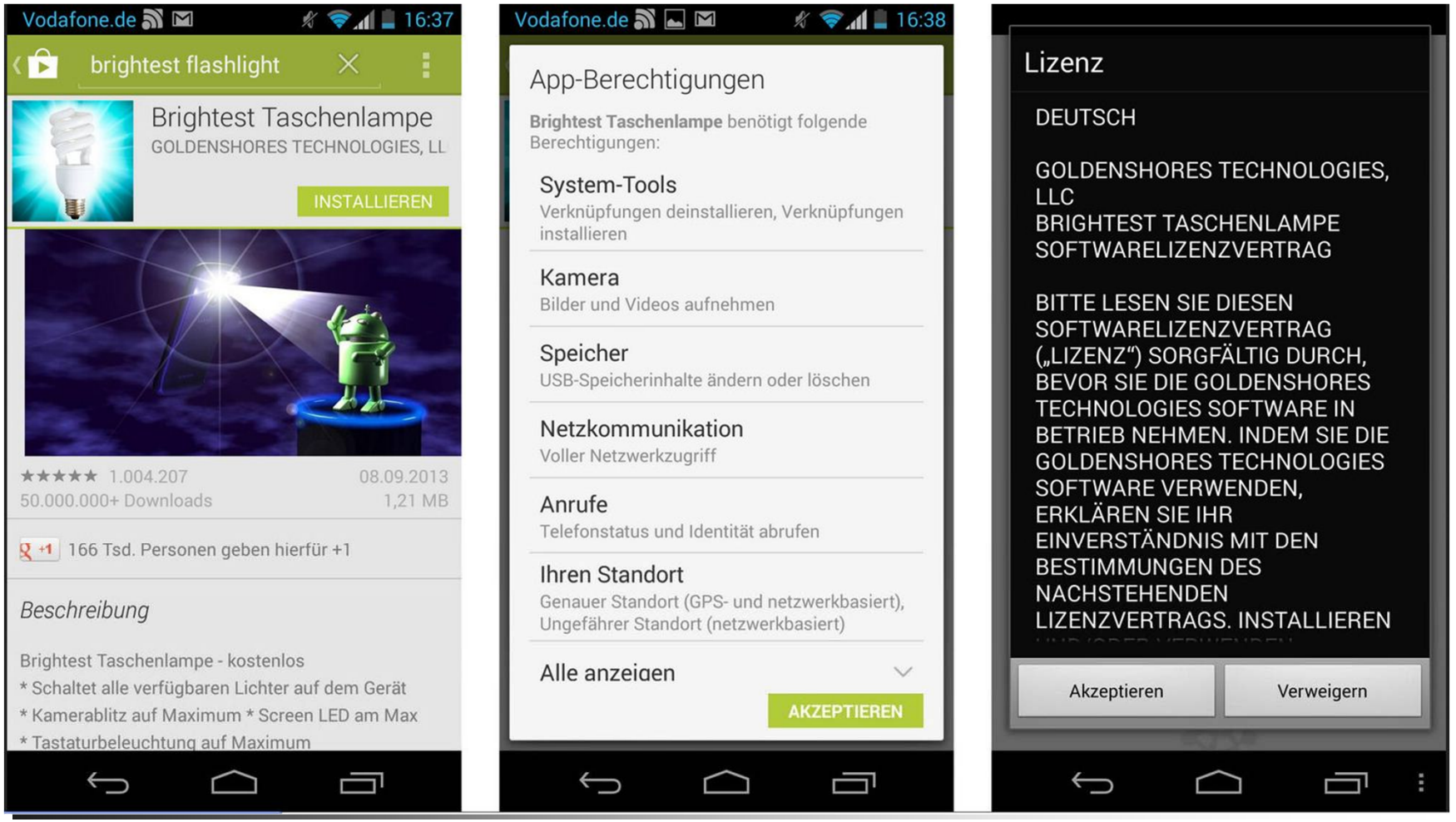
Geheimnisse

Unser Rechtssystem beruht auch auf Geheimnissen!

Grundgesetz:	- Brief-, Post- und Fernmeldegeheimnis
Strafgesetzbuch:	- Staatsgeheimnis
	- illegales Geheimnis
	- Wahlgeheimnis
	- Briefgeheimnis
	- fremdes Geheimnis
	- Postgeheimnis
	- Fernmeldegeheimnis
	- Dienstgeheimnis
	- Steuergeheimnis
Wirtschaftsrecht:	- Betriebs- und Geschäftsgeheimnis
Kirchenrecht:	- Beichtgeheimnis

Geheimnisse sind Friedenswahrer unserer Gesellschaft

„Aƀpp-gefahren“

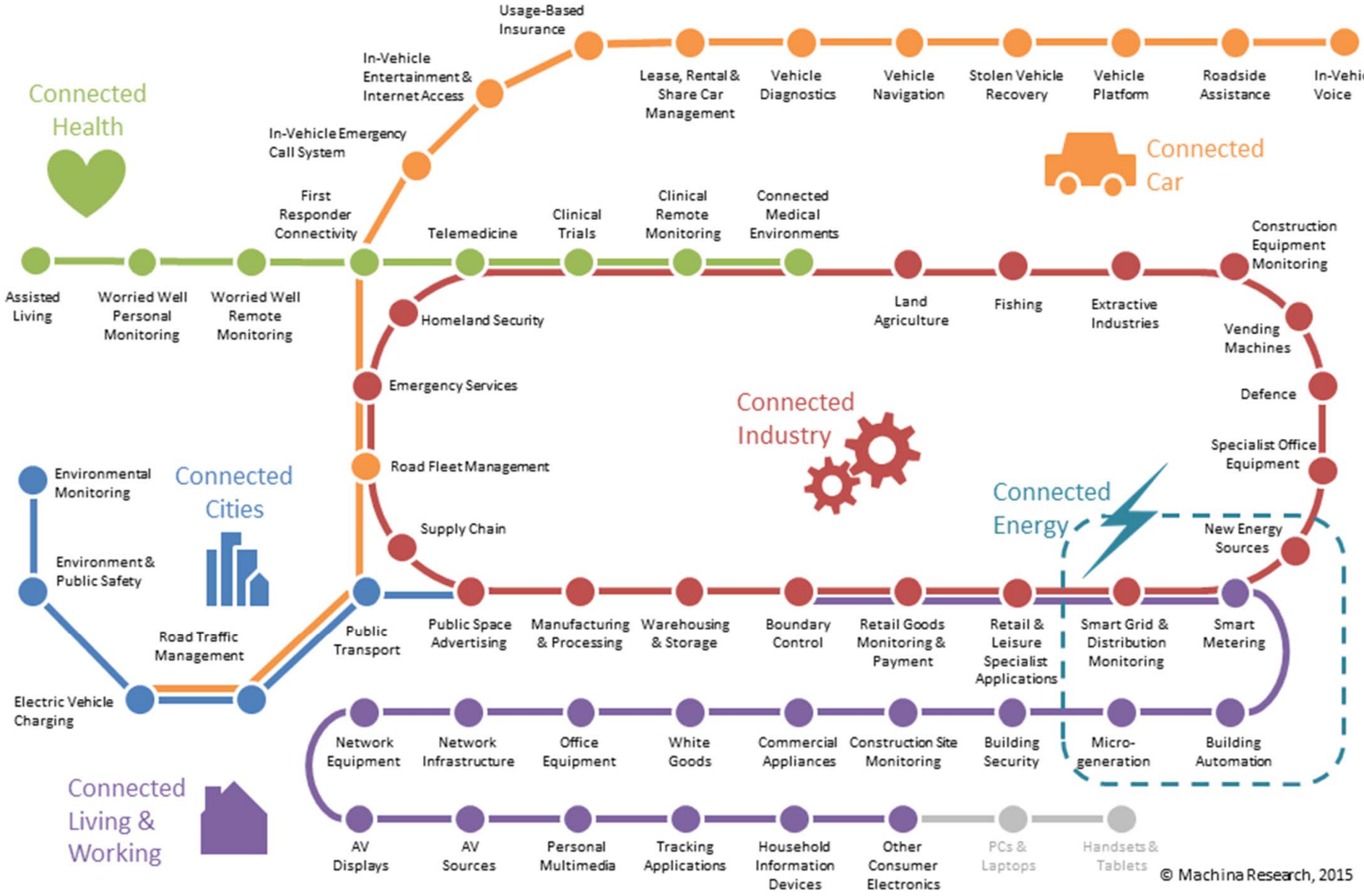


(einige) Beispiele für IoT Geräte und Anwendungen

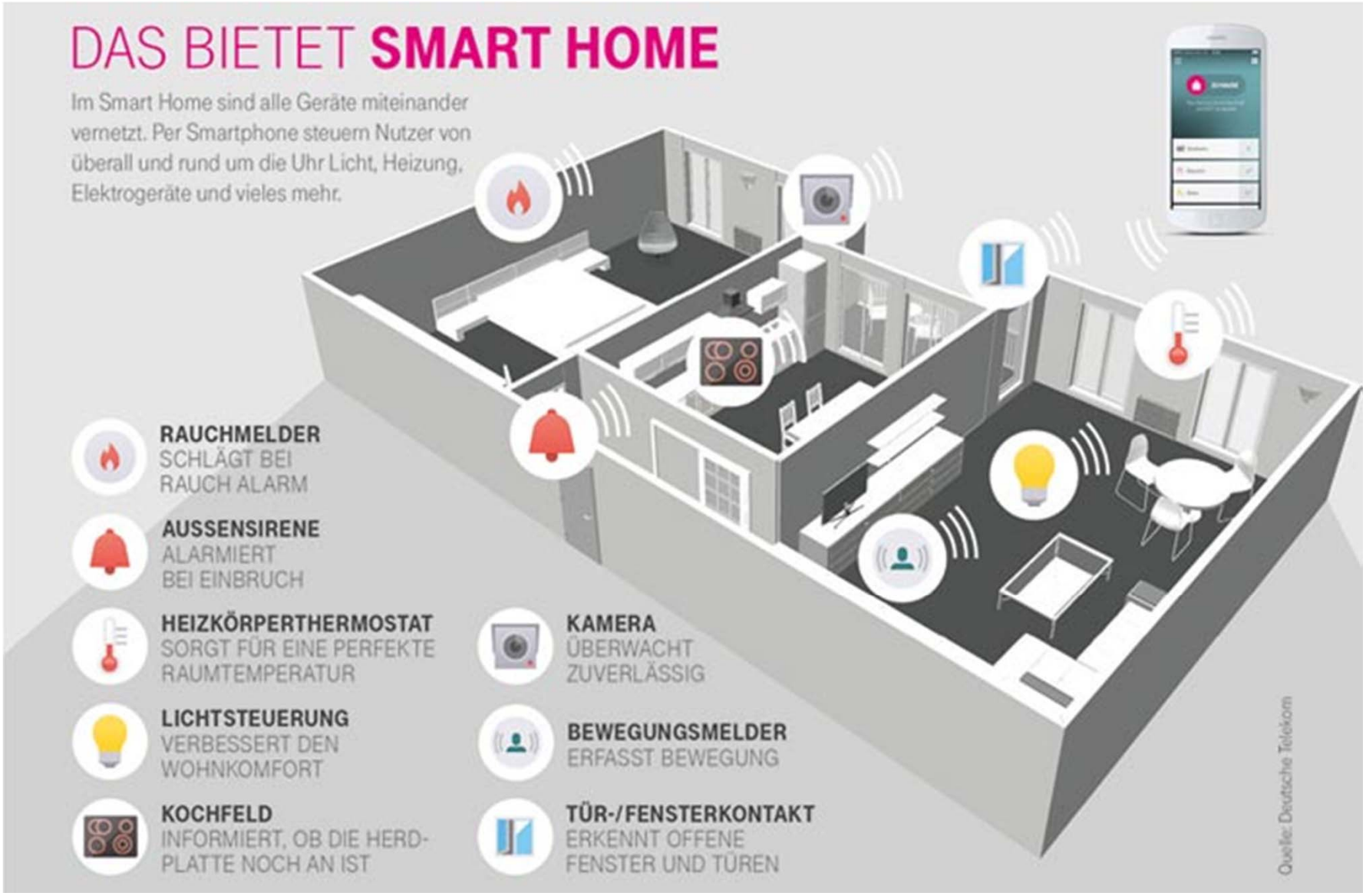
- Smart… Home/Cities/Car/Buildings/Transport/Grid/Toys…
- Digitale Selbstvermessung „Quantified Self“/Smart Health

  Life-Logging (Wearables): sportliche Leistung, Schlaftracking, Gesundheitszustand,…

  - Adidas kauft Runtatstic für 220 Million € (70 Millionen Nutzer; Fitbit beim Börsenstart 6 Mrd $ wert)
  - Runtastic: Datenverwendung „im Rahmen einer *sonstigen Aktivität* von Runtastic oder einem mit Runtastic verbundenen Unternehmen“ und „Recht der Veränderung und Bearbeitung, sofern nicht dadurch *berechtigte Interessen des Nutzers* beeinträchtigt werden“
  - HealthGraph-Daten (7 Mio. Nutzer) werden für Forschung verwendet; Angaben zu Forschungszweck und ob Anonymisierung: ???


Connected Health
Assisted Living
Worried Well Personal Monitoring
Worried Well Remote Monitoring
First Responder Connectivity
In-Vehicle Emergency Call System
In-Vehicle Entertainment & Internet Access
Usage-Based Insurance
Telemedicine
Clinical Trials
Clinical Remote Monitoring
Connected Medical Environments
Connected Car
Lease, Rental & Share Car Management
Vehicle Diagnostics
Vehicle Navigation
Stolen Vehicle Recovery
Vehicle Platform
Roadside Assistance
In-Vehicle Voice
Homeland Security
Emergency Services
Road Fleet Management
Supply Chain
Land Agriculture
Fishing
Extractive Industries
Construction Equipment Monitoring
Vending Machines
Defence
Specialist Office Equipment
Connected Industry
Connected Energy
New Energy Sources
Smart Metering
Smart Grid & Distribution Monitoring
Retail & Leisure Specialist Applications
Retail Goods Monitoring & Payment
Boundary Control
Warehousing & Storage
Manufacturing & Processing
Public Space Advertising
Public Transport
Environmental Monitoring
Environment & Public Safety
Connected Cities
Road Traffic Management
Electric Vehicle Charging
Network Equipment
Network Infrastructure
Office Equipment
White Goods
Commercial Appliances
Construction Site Monitoring
Building Security
Micro-generation
Building Automation
Connected Living & Working
AV Displays
AV Sources
Personal Multimedia
Tracking Applications
Household Information Devices
Other Consumer Electronics
PCs & Laptops
Handsets & Tablets
© Machina Research, 2015

Smart Home der Telekom



Smart Home: Hacker übernehmen Kontrolle über Thermostat

heise online 09.08.2016 19:32 Uhr – Volker Briegleb vorlesen

Dieses Thermostat heizt nur noch gegen Bitcoin. (Bild: Ken Munro auf Twitter)

Die Sicherheitsexperten Andrew Tierney und Ken Munro haben auf der Hacker-Konferenz Def Con gezeigt, wie sie ein "smartes" Thermostat kapern können. Wirklich schwer hat es ihnen die Hardware dabei nicht gemacht.

Auf der Hacker-Konferenz Def Con 24 in Las Vegas haben zwei Sicherheitsexperten gezeigt, wie sie ein vernetztes Thermostat eines ungenannten Herstellers mit einer Erpressungs-Software infizieren konnten. Den Hackern ist es gelungen, die Kontrolle über das Thermostat zu erlangen und die Funktionen für den Besitzer zu sperren. Theoretisch könnten Angreifer so zum Beispiel im Winter die Heizung abstellen, bis der arme Wohnungsinhaber zahlt.

"Armselige Sicherheit"

Verwundbare Autos

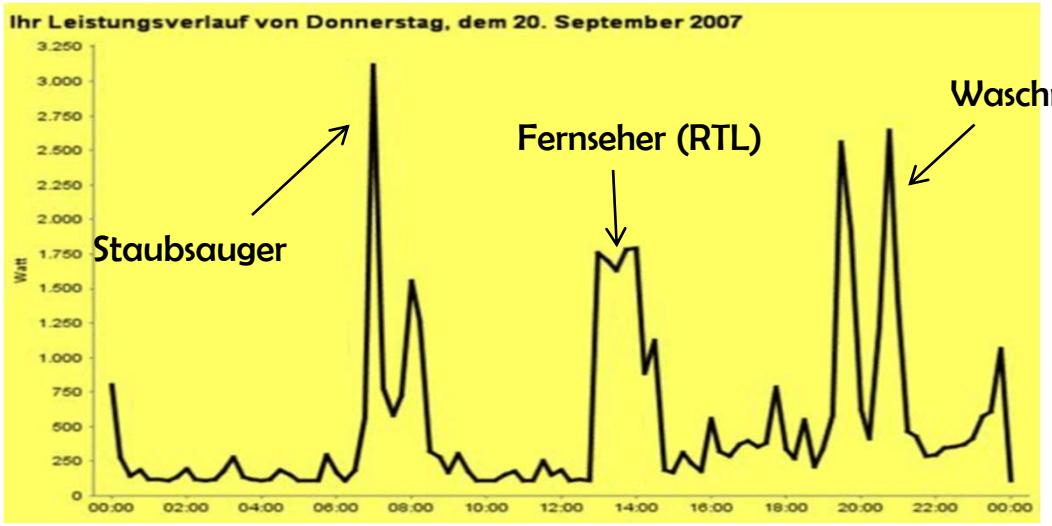
Wie zwei Hacker einen Jeep übernehmen

Mulmig war dem Journalisten Andy Greenberg, als sein Auto bei 110 Stundenkilometern gehackt wurde. Wenigstens wusste er grob, worauf er sich einlässt. Doch Besitzer smarter Autos dürften Bauchschmerzen bekommen.

22.07.2015, von FRIDTJOF KÜCHEMANN

Da hilft nur noch beten: Die elektronische Ausstattung macht den Jeep Cherokee attraktiv - und angreifbar.

Smart Meter



- differenzierte Verbrauchsmessung elektrischer Geräte
- eine Überwachung defekter elektrischer Geräte ("Pre-Maintenance")
- Zugriff auf einzelne elektrische Geräte auch aus der Ferne ("Remote Access")

Diese Informationen sind personenbezogen!

BLACK HAT EUROPE

Spanische Smart Meter können einfach gehackt werden

von Barbara Wimmer 16.10.14, 11:07 shroombab Mail an Autor

Symbolbild! Es wurde von den spanischen Sicherheitsforschern NICHT der Smart Meter dieses Herstellers gehackt. - Foto: Benjamin Sterbenz

BLACK HAT EUROPE

Spanische Smart Meter können einfach gehackt werden

KOMMENTARE (13)

MEHR ZUM THEMA

Spanische Sicherheitsforscher haben auf der Black Hat Europe einen Hack eines intelligenten Stromzählers gezeigt, mit dem ein Blackout verursacht werden kann.

SMART METERING, TU WIEN, SMART METER

In Spanien wurden bereits acht Millionen intelligente Stromzähler (Smart Meter) installiert, das sind rund 30 Prozent aller Haushalte. Zum Einsatz kommen dort Modelle der Firmen Endesa, Iberdrola und E.ON. Doch in Teilen Spaniens könnte es bald dunkel werden. Denn einer dieser Hersteller hat einen intelligenten Zähler im

Quelle: https://futurezone.at/

Alert!

IP-Kameras von Aldi als Sicherheits-GAU

15.01.2016 10:49 Uhr – Ronald Eikenberg

vorlesen

Aldi hatte vergangenes Jahr mehrfach IP-Überwachungskameras mit denkbar schlechten Voreinstellungen verkauft. Die Geräte sind zu Hunderten fast ungeschützt über das Internet erreichbar.

Die bei Aldi verkauften IP-Überwachungskameras der Marke Maginon haben massive Sicherheitsprobleme: Unbefugte könnten über das Internet auf das Kamerabild zugreifen und sogar den Ton anzapfen. Zudem verraten die Geräte unter anderem die Passwörter für WLAN, E-Mail und FTP-Zugang ihres Besitzers. Hunderte Aldi-Kameras sind nahezu ungeschützt über das Internet erreichbar. Darauf hat uns der Zusammenschluss Digitale Gesellschaft aufmerksam gemacht.

Betroffen ist unter anderem die Außenkamera IPC-20 C.

Bild: Hersteller

Drei Modelle sind betroffen

Die Kameras IPC-10 AC, IPC-100 AC und IPC-20 C hat

Quelle: https://www.heise.de

produkt WARNUNG

Start Blog App Impressum Produktrückruf melden Gesetze und Richtlinien Unterstützen

FOLGEN:

BLOG

Zum Suchen tippen und Enter drücken

UNTERSTÜTZEN & FÖRDERN

UNSERE MELDUNGEN

IM POSTFACH

Jetzt anmelden und alle Infos täglich kostenfrei per Mail erhalten

Email Adresse eingeben

Smartes Spielzeug: Spione im Kinderzimmer

VON REDAKTION · 28. AUGUST 2017

vernetztes Spielzeug

Vernetzte Roboter und Teddys sprechen mit ihren kleinen Besitzern und leider auch mit Internetservern.
Ihr harmloses Aussehen täuscht: Einige smarte Spielzeuge, die die Stiftung Warentest untersucht hat, entpuppten sich als Spione im Kinderzimmer. Bei zwei davon ist es Fremden sogar ohne großen technischen Aufwand möglich, sie aus der Nachbarwohnung fernzusteuern und darüber mit Kindern zu kommunizieren. Schuld sind unsichere Funkverbindungen.

Drei der sieben geprüften Spielzeuge sind sehr kritisch, die anderen vier kritisch, so die September-Ausgabe des Magazins test.

Quelle: https://www.produktwarnung.eu

Internet of ~~Things~~ Bots?

Aussage von John Adams:

- „Es gibt kein Internet der Dinge. Es gibt nur viele ungepatchte, verwundbare, kleine Computer im Internet.“

DDoS Angriffe aus dem IoT in neuen Dimensionen

Auf den Blog von Brian Krebs wurde ein DDoS Angriff mit einem Rekord-Traffic von 620 Gigabit pro Sekunde bekannt. Doch die nächste Rekordmeldung ließ nicht lange auf sich warten. Vorletzte Woche erschienen Meldungen über einen Angriff aus vermutlich derselben Quelle mit bis zu 1,1 Terabit pro Sekunde auf den französischen Web Hoster OVH. Die beiden erreichten Übertragungsraten übertrafen alle jemals zuvor dokumentierten DDoS Angriffe. Das verwendete Botnetz war bisher nicht bekannt und soll aus über 150.000 IoT-Systemen wie IP-Kameras und Festplatten-Receivern bestanden haben. Diese sind oft schlecht abgesichert und stellen somit ein leichtes Angriffsziel dar. Da die eigentliche Funktion der Geräte bei einem Befall mit Malware in der Regel nicht spürbar beeinträchtigt wird, bleiben die Infektionen in vielen Fällen unentdeckt. Brian Krebs schreibt in seinem Blog, dass es sich um eine Malware namens „Mirai“ handelt, deren Quellcode vor kurzem öffentlich geworden ist. „Mirai“ nutzt zur Übernahme der Geräte einen vergleichsweise einfachen Weg: Die Software scannt nach Geräten im Internet und versucht, sich mit den Standardbenutzern und Passwörtern der Hersteller an den Geräten anzumelden und sich im Anschluss auf diesen einzunisten.

Baden-Württemberg
DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ

PRESSEMITTEILUNG 22. September 2016

Datenschutz beim „Internet der Dinge“ – Klein und nicht fein!

Unter dem Titel „GPEN Privacy Sweep 2016“ hat die englische Datenschutzaufsichtsbehörde eine Aktion zur Prüfung des Datenschutzes bei Produkten im Bereich des „Internet der Dinge“ bzw. „Internet of Things“ (IoT) angestoßen und koordiniert. GPEN steht für „Global Privacy Enforcement Network“ und ist ein informeller Zusammenschluss von Datenschutzaufsichtsbehörden auf der ganzen Welt. An der diesjährigen Prüfung haben 25 der im GPEN aktiven Datenschutzaufsichtsbehörden teilgenommen. Auch der Landesbeauftragte für den Datenschutz Baden-Württemberg hat sich an der Aktion beteiligt und Produkte untersucht, die in Baden-Württemberg entwickelt werden.

Immer mehr elektronische Produkte sind heutzutage mit dem Internet verbunden - von Steuergeräten für das „Smart Home“ über Fitness Tracker oder Pulsmesser bis hin zum Smart TV. Dank miniaturisierter Sensoren wird eine Vielzahl physikalischer oder biomedizinischer Größen durch diese „intelligenten“ Geräte erfasst. Gesteuert werden sie häufig per App auf dem Smartphone. So lässt sich beispielsweise die Heizung im Smart Home von überall auf der Welt per App ein- und ausschalten. Auch

Beschluss der 206. IMK vom 14.06.2017

1. Die IMK stellt fest, dass die massenhafte Verbreitung von mit dem Internet verbundenen Gebrauchsgeräten (Internet der Dinge) ohne ausreichende Sicherheitsvorkehrungen eine erhebliche Bedrohung für den Cyberraum darstellt.

2. Sie hält eine Intensivierung der Maßnahmen zur Verbesserung der Cybersicherheit bezogen auf das Internet der Dinge für erforderlich. Dies sollte im Rahmen eines umfassenden Handlungskonzepts erfolgen, das unter anderen folgende Themenfelder adressiert wie:

   a) Schaffung verbindlicher Produktsicherheitsstandards für mit dem Internet verbundene Geräte,

   b) Schaffung von Regelungen zur Produkthaftung für mit dem Internet verbundene Geräte unter Berücksichtigung von IT-spezifischen Schadensfällen.

3. Die IMK bittet die länderoffene Arbeitsgruppe Cybersicherheit, diese Thematik umfassend zu prüfen und hierbei den IT-Planungsrat im erforderlichen Umfang zu beteiligen.

(Kurz-)Fazit

- DPIA – Data Protection Privacy Assessment (Art. 35 DSGVO)
- Privacy by Design und Privacy by Default (Art. 25)
- Datenminimierung: so wenig Daten wie nötig, Rohdaten frühestmöglich und am dichtesten Punkt (am „Smart Device“) löschen, Daten aggregieren wenn möglich (Art. 5)
- Einsatz verschlüsselter Kommunikation; ggf. Entwicklung neuer Verschlüsselungsalgorithmen notwendig
- nutzerfreundliche Informationspflichten / Einwilligungen (Art. 7)
- feingranulare „Datensteuerung“ ermöglichen (opt-out und abschalten von einzelnen Funktionen)
- Zertifizierung und Auditierung von Produkten und Verfahren (Art. 42)
- Data Breach Notifications (Infos über Datenlecks und Anleitungen) (Art. 34)

Vielen Dank für Ihre Geduld!

Quelle: Pixabay